A Flexible Security Architecture for Ubiquitous Mobile & Wearable Systems

John Murray PhD CEng
PEMSTAR Pacific Consultants, San Jose CA
+1-408-282-4805
jxm@pacificconsultants.com

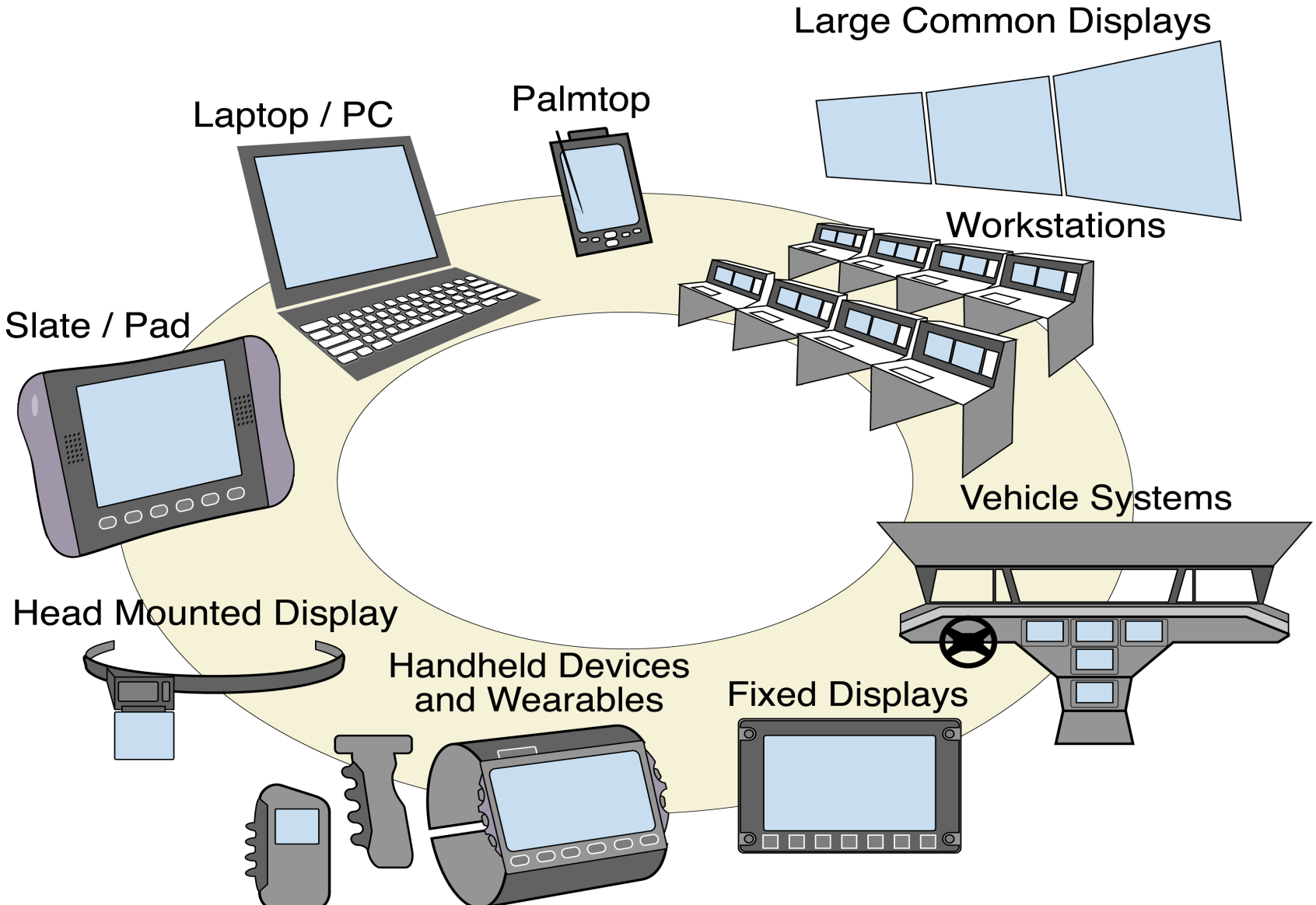
PEMSTAR
PACIFIC CONSULTANTS

Overview

- Ubiquitous Computing
- Mobile Ad-Hoc Networks (MANET)
- User Interactions with Wearable Systems
- Security & Role-Based Access Control
- Wearable Systems Security Issues
- Intrusion Detection in Wireless Networks
- Questions & Comments

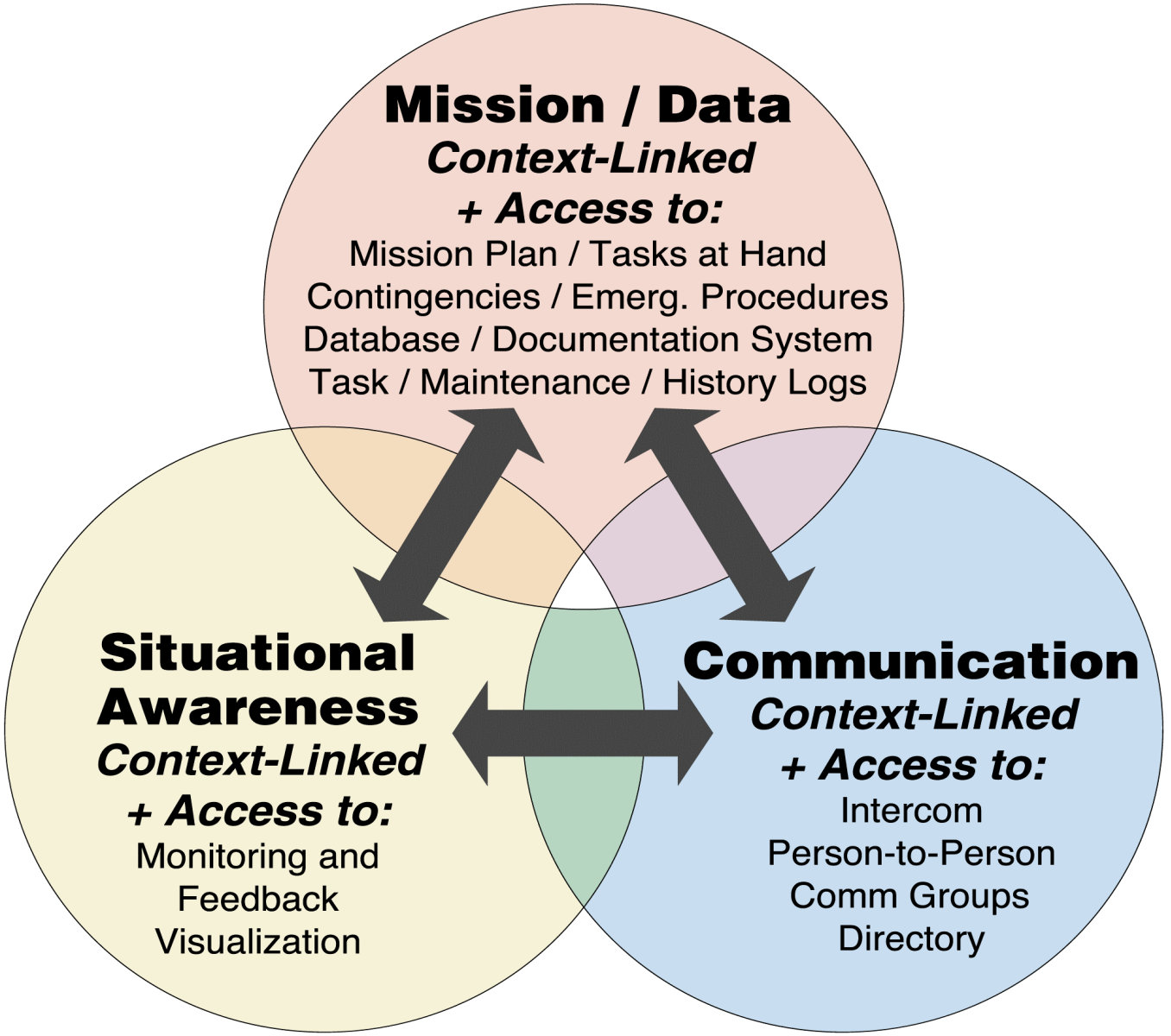
PEMSTAR
PACIFIC CONSULTANTS

Ubiquitous Computing



PEMSTAR
PACIFIC CONSULTANTS

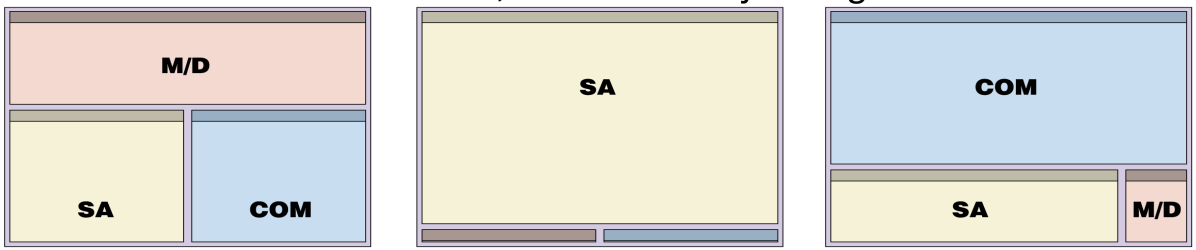
Contextual Cross-Links



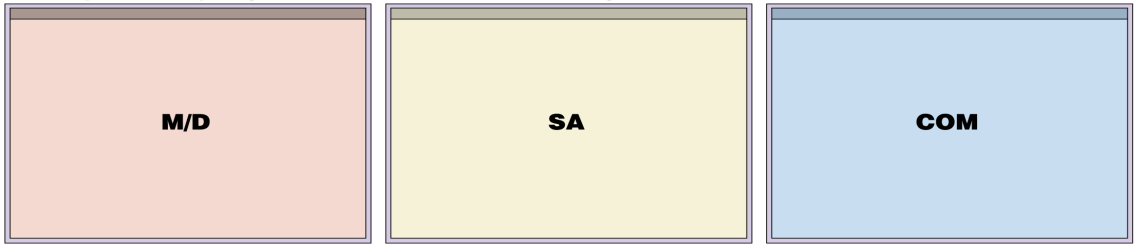
PEMSTAR
PACIFIC CONSULTANTS

Flexible Interactional Architecture

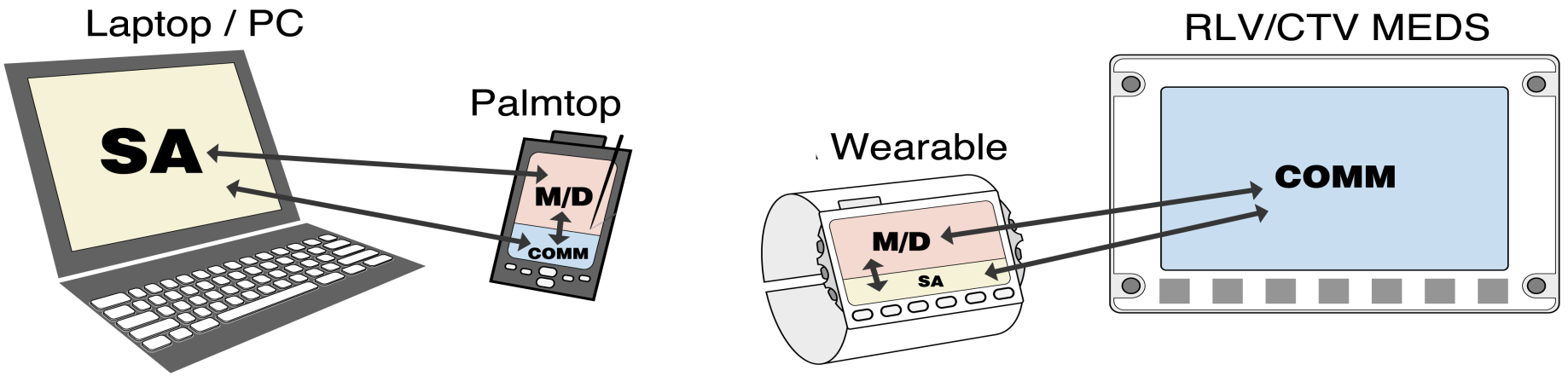
Screen Divisions are not fixed, but are flexibly configurable



Multiple Displays can be Contextually Linked

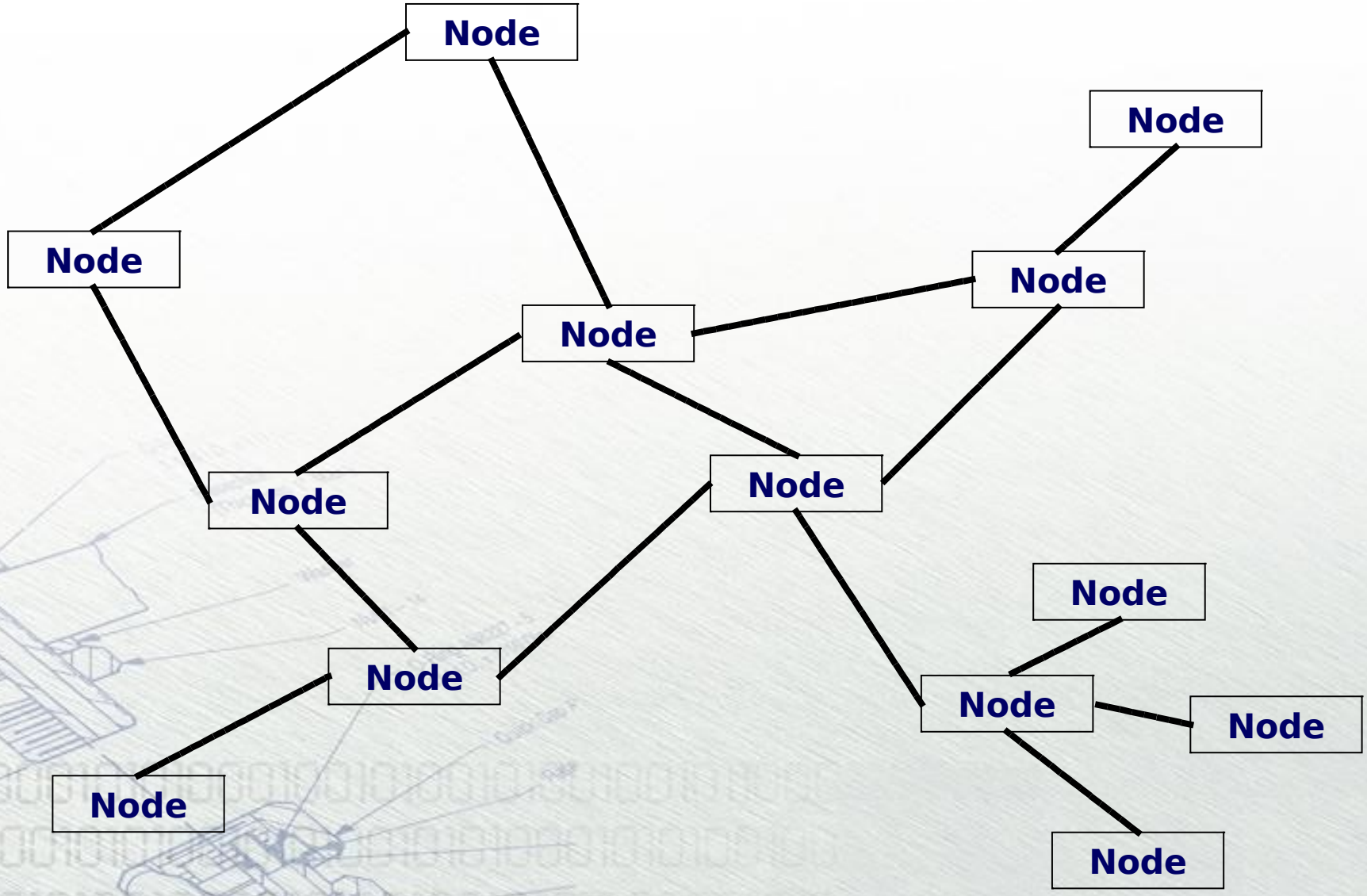


Devices Can Be Linked On The Fly To Link Up Contextually



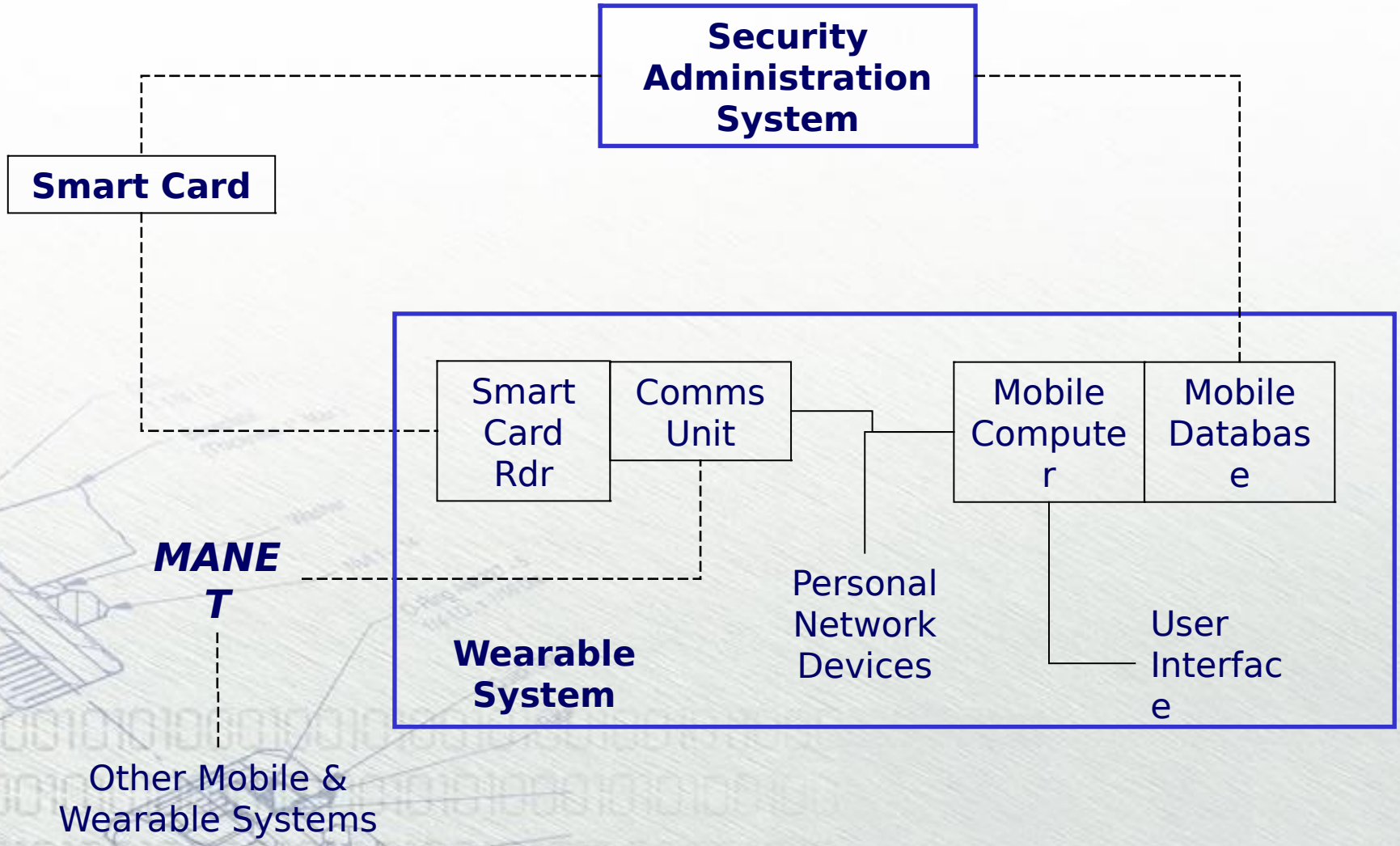
PEMSTAR
PACIFIC CONSULTANTS

Mobile Ad-hoc Networks (MANET)



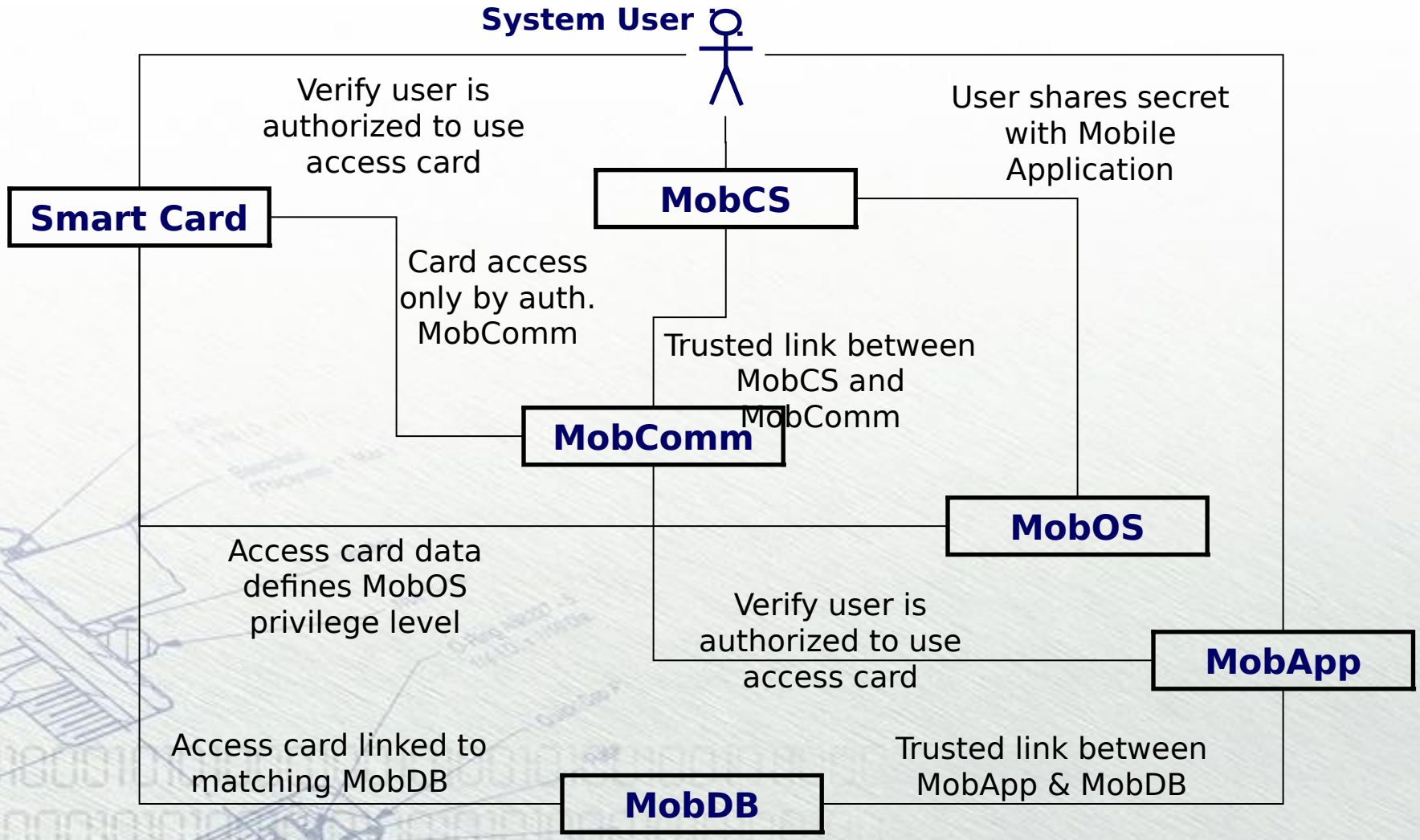
PEMSTAR
PACIFIC CONSULTANTS

Wearable Systems Individual Architecture



PEMSTAR
PACIFIC CONSULTANTS

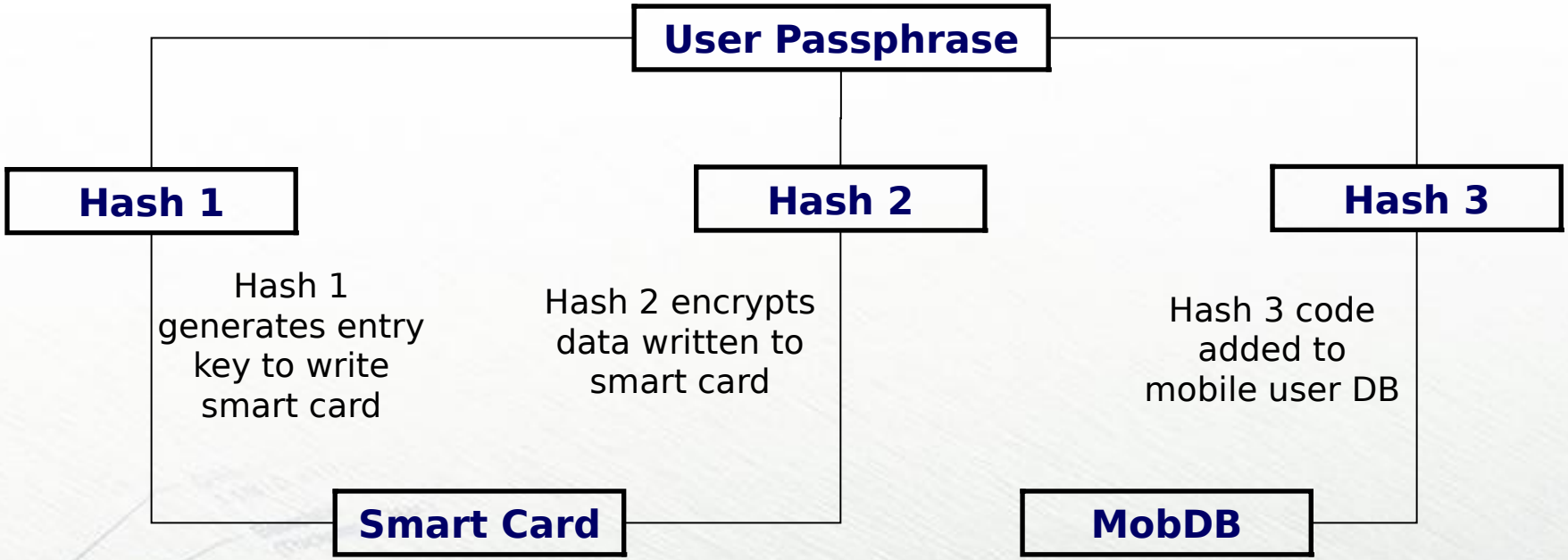
Security Issues on Wearable Systems


System User
Verify user is authorized to use access card
User shares secret with Mobile Application
Smart Card
MobCS
Card access only by auth. MobComm
Trusted link between MobCS and MobComm
MobComm
MobOS
Access card data defines MobOS privilege level
Verify user is authorized to use access card
MobApp
Access card linked to matching MobDB
Trusted link between MobApp & MobDB
MobDB

Patent Pending

PEMSTAR
PACIFIC CONSULTANTS

User Passphrase Management

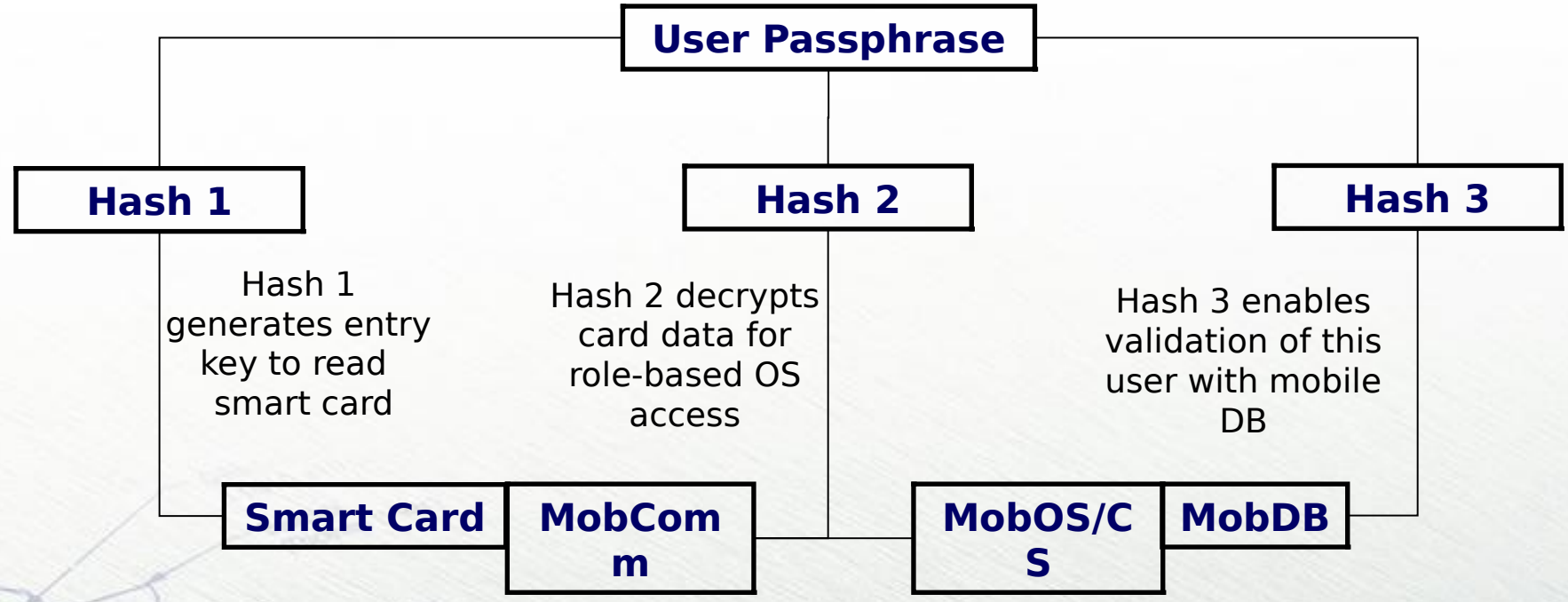

User Passphrase
Hash 1
Hash 2
Hash 3
Hash 1 generates entry key to write smart card
Hash 2 encrypts data written to smart card
Hash 3 code added to mobile user DB
Smart Card
MobDB

- **Security Administration System**
  - User provides personal secret data (“passphrase”)
  - Derive two elements to generate card write & encrypt keys
  - Additional elements for inclusion in mobile user database

Patent Pending

PEMSTAR
PACIFIC CONSULTANTS

Passphrase Usage Process

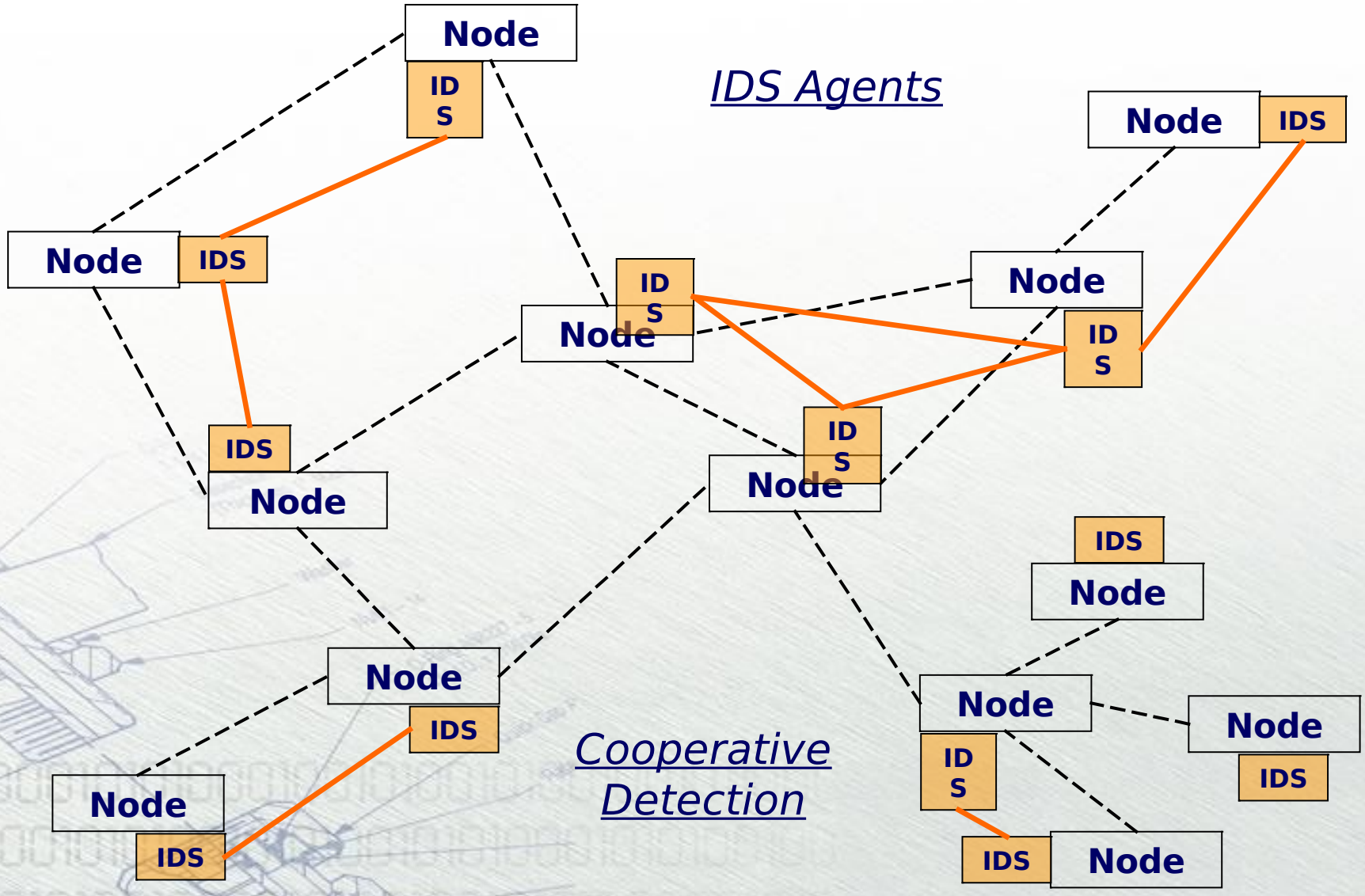


- **Mobile Wearable System**
  - User provides passphrase and presents smart card
  - Role-based card data provides access to MobOS & MobCS
  - Secret shared with mobile application and database

Patent Pending

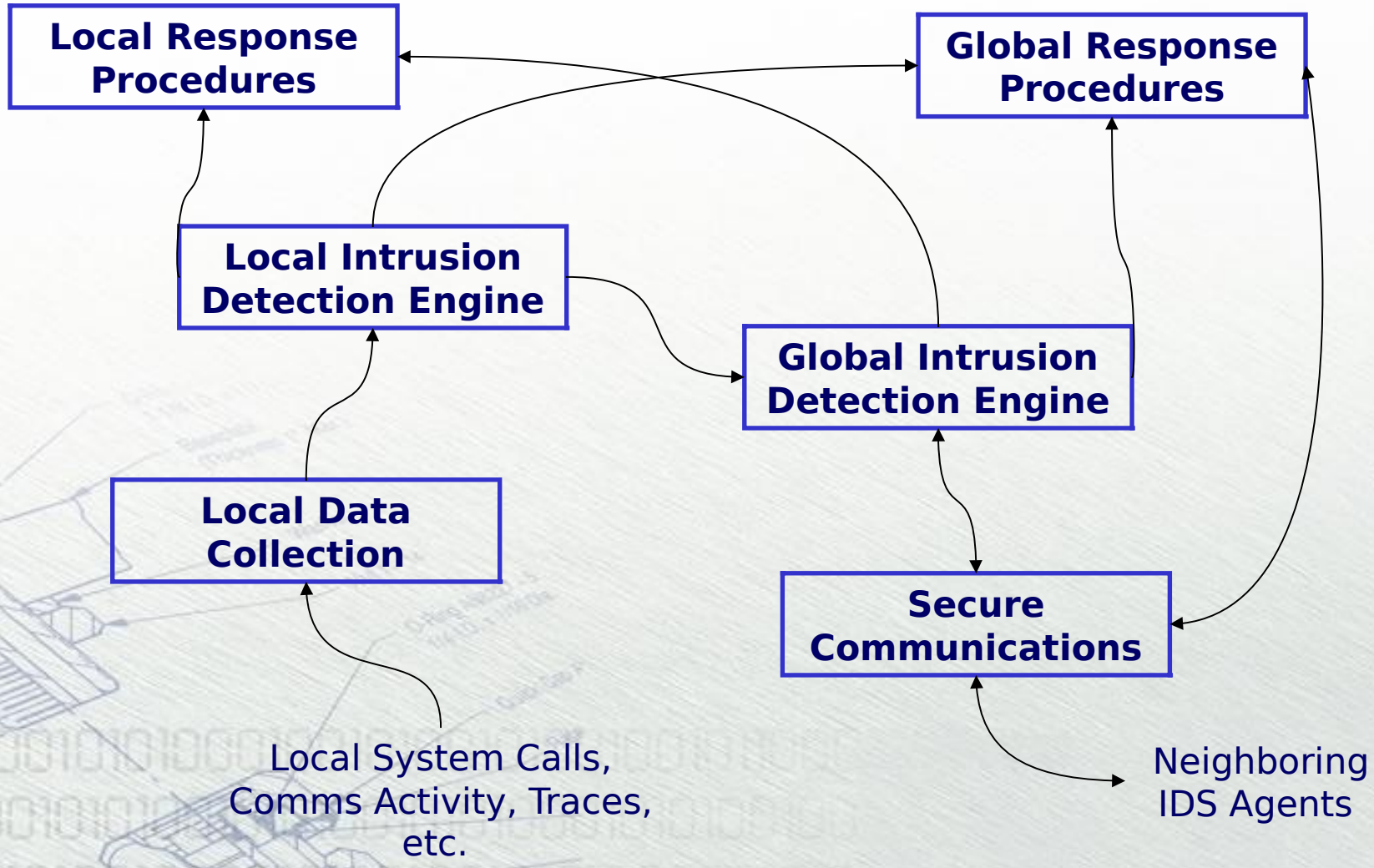
PEMSTAR
PACIFIC CONSULTANTS

MANET Security



PEMSTAR
PACIFIC CONSULTANTS

Intrusion Detection System (IDA) Agent



PEMSTAR
PACIFIC CONSULTANTS

For Additional Information.....

- Weiser M: “The Computer for the Twenty-First Century”, Scientific American, v265-3, Sept. 1991.
- Kindberg T & Fox A, “System Software for Ubiquitous Computing”, IEEE Pervasive Computing, Jan-Mar 2002.
- Murray J, Leftwich J & Munro P: “A Contextually-Integrated Human Interface Architecture For Mobile & Wearable Systems”, Land Warfare Conference, Brisbane Australia, 2002.
- Pemstar Pacific Consultants, “A Flexible Security Architecture for Ubiquitous Mobile & Wearable computers”, US Patent Application Documentation, 2004.
- Zhang Y, Lee W & Huang Y: “Intrusion Detection Techniques for Mobile Wireless Networks”, ACM Wireless Networks, 9, 2003.

PEMSTAR
PACIFIC CONSULTANTS

A Flexible Security Architecture for Ubiquitous Mobile & Wearable Systems

John Murray PhD CEng

PEMSTAR Pacific Consultants, San Jose CA

+1-408-282-4805

jxm@pacificconsultants.com